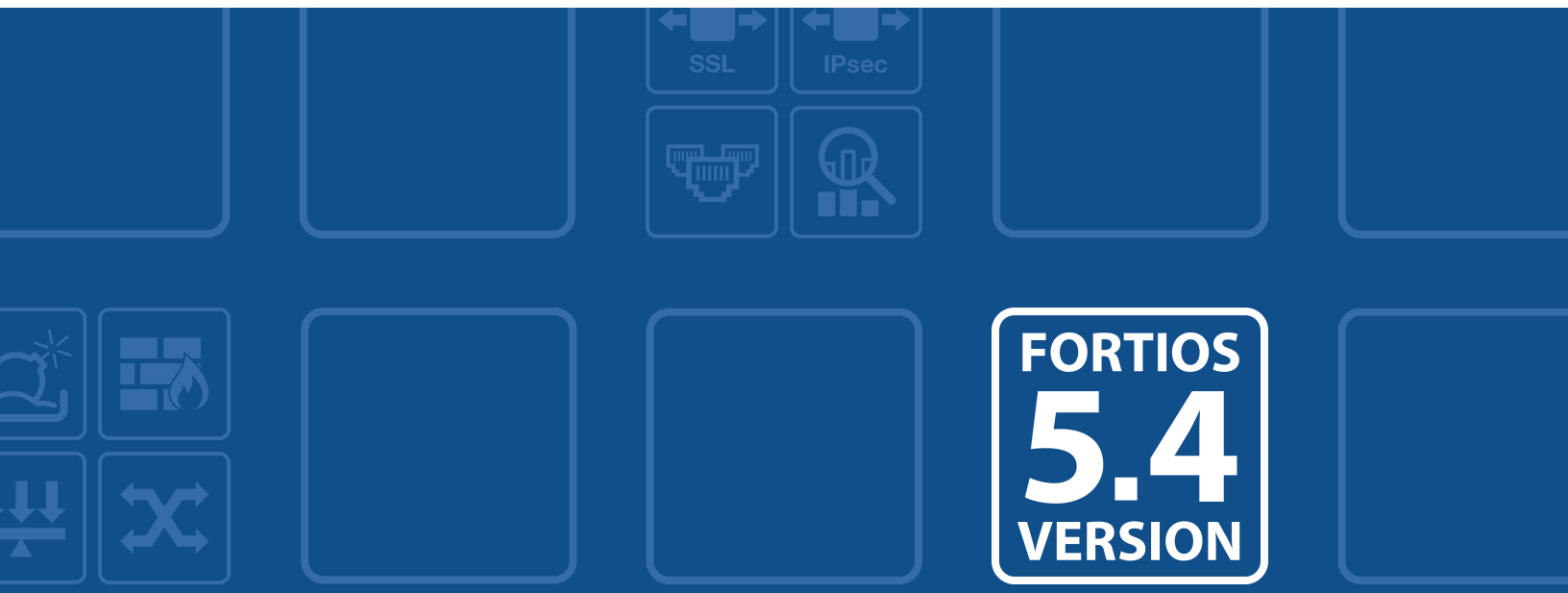
FORTINET
High Performance Network Security

ADMINISTRATION GUIDE

# Managed FortiSwitches Using FortiGate

for FortiOS 5.4 and FortiSwitchOS 3.x




FORTIOS
5.4
VERSION

**FORTINET DOCUMENT LIBRARY**

http://docs.fortinet.com

**FORTINET VIDEO GUIDE**

http://video.fortinet.com

**FORTINET BLOG**

https://blog.fortinet.com

**CUSTOMER SERVICE & SUPPORT**

https://support.fortinet.com

http://cookbook.fortinet.com/how-to-work-with-fortinet-support/

**FORTIGATE COOKBOOK**

http://cookbook.fortinet.com

**FORTINET TRAINING SERVICES**

http://www.fortinet.com/training

**FORTIGUARD CENTER**

http://www.fortiguard.com

**END USER LICENSE AGREEMENT**

http://www.fortinet.com/doc/legal/EULA.pdf

**FEEDBACK**

Email: techdocs@fortinet.com

Tuesday, January 05, 2016

Managed FortiSwitches Using FortiGate

for FortiOS 5.4 and FortiSwitchOS 3.x

# TABLE OF CONTENTS


**Change Log** ..... **5**
**Introduction** ..... **6**
Supported Models ..... 6
Before You Begin ..... 7
How this Guide is Organized ..... 7
**Initial Set-up** ..... **8**
Enable the Switch Controller on FortiGate ..... 8
Connect the FortiSwitch and FortiGate ..... 8
Auto-discovery of the FortiSwitch Ports ..... 8
Choosing the FortiGate Ports ..... 9
Configuring FortiLink (Single Link) ..... 10
Configuring the switch ..... 10
Configuring the Port and Authorizing the FortiSwitch ..... 10
Using the CLI ..... 11
Configuring FortiLink (LAG) ..... 12
Configuring the switch ..... 12
Configuring the LAG on the FortiGate ..... 13
Using the FortiGate CLI ..... 14
Configuring FortiSwitch Management Port ..... 15
Converting to FortiSwitch Standalone Mode ..... 15
**VLAN Configuration** ..... **17**
FortiSwitch VLANs Display ..... 18
Creating VLANs ..... 18
Using the web-based manager ..... 18
Using the CLI ..... 19
Setting up a security policy for the VLAN ..... 20
Using the web-based manager ..... 20
Using the CLI ..... 20
**FortiSwitch Port and POE Configuration** ..... **22**
FortiSwitch Ports Display ..... 22
Configuring Ports Using the Web Manager ..... 23
Configure Native VLAN on a port ..... 23
Configure Allowed VLANs on a port ..... 23
Enable or Disable POE on a port ..... 23
Configuring Ports Using the CLI ..... 24
Port commands ..... 24
POE commands ..... 24
**Configuring FortiLink for FortiGate HA** ..... **25**
Example Topology ..... 25

Adding a Second FortiGate to Existing Single FortiGate 26
Configuration Steps 26
Adding a Switch to Existing HA FortiGates (single FortiLinks) 26
Configuration Steps 26
Adding a Switch to Existing FGT HA setup (Fortilink LAGs) 27
Configuration Steps 27
Create VLANs for LAN and WAN ports 27
Test the HA Capability 27
Display FortiSwitch Port Statistics 27
**Troubleshooting 29**
Troubleshooting FortiLink Issues 29
Check the FortiGate configuration 29
Check the FortiSwitch configuration 29
**Scenarios 30**
The Example Network 30
Scenario 1: Allowing access to specific users on the marketing VLAN 31
Using the web-based manager 32
Using the CLI 34
Scenario 2: Adding a specific device to the marketing VLAN 35
Using the web-based manager 35
Using the CLI 36

# Change Log

| Date | Change Description |
|---|---|
| April 20, 2015 | Initial document release (FortiOS 5.2.1 and FortiSwitchOS 3.0.1) |
| July 23, 2015 | Updates for FortiOS 5.4 and FortiSwitchOS 3.3.0. |
| Aug 18, 2015 | Clarify that Fortilink LAG is not limited to 2 links. |
| Sept 18, 2015 | Update the list of FortiGate models that are supported in FortiOS 5.4.0 |
| Oct 22, 2015 | Add the new FortiGate models into the table on page 10 (their FortiLink ports) |
| Nov 24, 2015 | Updates to reflect new features in the FortiGate 5.4 web manager. |
| Dec 14, 2015 | Updated the FortiLink product matrix. |

# Introduction

This document provides information about how to setup and configure Managed FortiSwitches with a FortiGate. This is also known as using FortiSwitch in Fortilink mode.

The following new Fortilink features are available starting in FortiOS 5.4.0 and FortiSwitchOS 3.3.0:

- POE configuration
- High Availability mode
- Fortilink Link Aggregation Group (LAG)
- Auto-detect Fortilink ports on the FortiSwitch.

## Supported Models

The following table shows the FortiSwitch models that support Fortilink mode when paired with the corresponding FortiGate models and the listed minimum software releases.

| FortiGate Models | Earliest FortiOS | FortiSwitch Models |
|---|---|---|
| FGT-90D | 5.2.2 | FS-224D-POE |
| FGT-60D<br>FGT-90D<br>FGT-100D, FGT-140D (POE, T1)<br>FGT-200D, FGT-240D, FGT-280D (POE)<br>FGT-600C<br>FGT-800C<br>FGT-1000C | 5.2.3 | FSR-112D-POE<br>FS-108D-POE<br>FS-124D<br>FS-124D-POE<br>FS-224D-POE<br>FS-224D-FPOE |
| | 5.4.0 | All FortiSwitch D-series models |
| FGT-1200D<br>FGT-1500D<br>FGT-3700D<br>FGT-3700DX | 5.4.0 | All FortiSwitch D-series models |

## Before You Begin

Before you configure the managed FortiSwitch unit, the following assumptions have been made in the writing of this manual:

- You have completed the initial configuration of the FortiSwitch unit, as outlined in the QuickStart Guide for your FortiSwitch, and you have administrative access to the FortiSwitch web-based manager and CLI.
- You have installed a FortiGate unit on your network and have administrative access to the FortiGate web-based manager and CLI.

## How this Guide is Organized

This guide contains the following sections:

Initial Set-up - describes how to set up the FortiSwitch to be managed by a FortiGate unit.

VLAN Configuration - configure VLANs from the FortiGate unit.

FortiSwitch Port and POE Configuration - configure Ports and POE from the FortiGate unit.

Configuring Fortilink for FortiGate HA - how to configure Fortilink when you have a pair of FortiGate units in HA mode.

Scenarios - contains practical examples of how to use managed FortiSwitch units in a network.

# Initial Set-up

This section describes the initial configuration and set-up for managing FortiSwitch with a FortiGate unit.

## Enable the Switch Controller on FortiGate

Prior to connecting the FortiSwitch and FortiGate units, enable the Switch Controller menu on the FortiGate. Use the FortiGate web-based manager or CLI to enable the Switch Controller.

### Using the FortiGate web-based manager

1. Go to **System > Features**.
2. Turn on the **Switch Controller** feature.
3. Select **Apply**.

The menu option **WiFi & Switch Controller** now appears in the web-based manager.

### Using the FortiGate CLI

Use the following command to enable the Switch Controller and set the reserved subnetwork for the controller:

```
config system global
   set switch-controller enable
   set switch-controller-reserved-network 169.254.254.0 255.255.255.0
end
```

## Connect the FortiSwitch and FortiGate

In FortiSwitchOS 3.3.0 and later releases, FortiSwitchOS provides additional flexibility for FortiLink, when used in conjunction with FortiOS 5.4 :

- Use any switch port for FortiLink
- Provides auto-discovery of the FortiLink ports on the FortiSwitch
- Choice of a single FortiLink port or multiple FortiLink ports in a link-aggregation group (LAG)

### Auto-discovery of the FortiSwitch Ports

In releases FortiSwitchOS 3.3.0 and beyond, the D-series FortiSwitch models support FortiLink auto-discovery, which is automatic detection of the port connected to the FortiGate.

You can use any of the switch ports for FortiLink. Use the following commands to configure a port for FortiLink auto-discovery:

```
config switch interface
   edit <port>
   set auto-discovery-fortilink enable
end
```

**NOTE**: Complete this configuration step BEFORE connecting the switch to the FortiGate.

Each FortiSwitch model provides a set of ports that are enabled for FortiLink auto-discovery by default. If you connect the FortiLink using one of these ports, no switch configuration is required.

The general rule (in FortiSwitchOS 3.4.0 and later releases) is that the last four copper ports are the default auto-discovery FortiLink ports. You can also run the **show switch interface** CLI command on the FortiSwitch to see the ports that have auto-discovery enabled.

The table below lists the default auto-discovery ports for each switch model:

| FortiSwitch Model | Default Auto-FortiLink ports |
|---|---|
| FS-108D | ports 9 and 10 |
| FSR-112D | ports 9, 10, 11 and 12 |
| FS-224D-POE | ports 21, 22, 23 and 24 |
| FS-1024D, FS-1048D, FS-3032D | all ports |
| FS-124D, FS-124D-POE | ports 23, 24, 25 and 26 |
| FS-224D-FPOE | ports 25, 26, 27 and 28 |
| FS-424D-FPOE | ports 25 and 26 |
| FS-524D-FPOE | ports 25, 26, 27, 28, 29 and 30 |
| FS-548D-FPOE | ports 49, 50, 51, 52, 53 and 54 |
| FS-248D-FPOE | ports 49, 50, 51, and 52 |
| FS-524D | ports 25, 26, 27, 28, 29 and 30 |
| FS-548D | ports 49, 50, 51, 52, 53 and 54 |

## Choosing the FortiGate Ports

For all FortiGate models, you can connect up to 16 FortiSwitches to one FortiGate unit.

The following table shows the ports for each model of FortiGate that you can use for FortiLink.

| FortiGate Model | Ports for Fortilink connection |
|---|---|
| FGT-60D, FGT-60D-POE<br>FWF-60D, FWF-60D-POE | port1 - port7 |

| FortiGate Model | Ports for Fortilink connection |
|---|---|
| FGT-90D, FGT-90D-POE<br>FWF-90D, FWF-90D-POE | port1 - port14 |
| FGT-100D | port1 - port16 |
| FGT-140D , 140D-POE, 140D-POE-T1 | port1 - port36 |
| FGT-200D | port1 - port16 |
| FGT-240D | port1 - port40 |
| FGT-280D, FGT-280D-POE | port1 - port84 |
| FGT-600C | port3 - port22 |
| FGT-800C | port3 - port24 |
| FGT-1000C | port3 - port14, port23 - port24 |
| FGT-1200D | port1 - port36 |
| FGT-1500D | port1 - port40 |
| FGT-3700D, FGT-3700DX | port1 - port32 |

# Configuring FortiLink (Single Link)

The following sections describe how to configure FortiLink using a single switch port.

## Configuring the switch

No additional switch configuration is required for FortiLink.

## Configuring the Port and Authorizing the FortiSwitch

Configure the FortiLink port on the FortiGate, and authorize the FortiSwitch as a managed switch.

**Using the web-based manager**

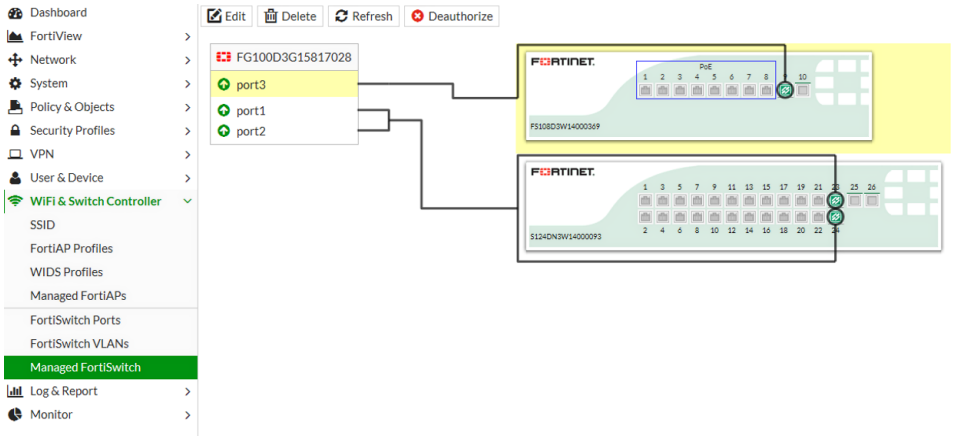
1. Go to **System** > **Network** > **Interfaces**
2. (Optional) If the FortiLink physical port is currently included in the internal interface, edit the internal interface and remove the desired port from the Physical Interface Members.
3. Edit the FortiLink port.
4. Enter the following fields in the **Edit Interface** form:
   a. **Addressing mode**: Set to **Dedicate to Extension Device**.
   b. **IP/Network Mask**: system automatically sets the IP address and network mask.

c. (Optional) **Automatically authorize devices**: disable to manually authorize the FortiSwitch.
d. Select **OK**.

5. Go to **WiFi & Switch Controller** > **Managed FortiSwitch**.
6. (Optional)Click on the FortiSwitch faceplate and click **Authorize**. This step is required only if you disabled the automatic authorization field of the interface.

The following image shows the Managed FortiSwitch display. The page displays the FortiGate ports on the left, and the faceplate for each switch on the right.

When the FortiLink is established successfully, the port status is green (on the FortiGate port and on the FortiSwitch faceplate) and the link between the ports is a solid line.




In **System** > **Network** > **Interfaces**, the system displays the switch ID next to the interface name, and displays **Dedicated to Extension Device** in the IP/Netmask field .

**Note**: An interface configured for managed FortiAP is also set to **Dedicated to Extension Device**. Make sure that you are viewing the correct FortiLink interface.

## Using the CLI

In the following steps, port1 is configured as the FortiLink port.

1. If required, remove port 1 from the **lan** interface:

```
config system virtual-switch
   edit lan
      config port
         delete port1
      end
   end
end
```

2. Configure the interface for port 1.

```
config system interface
   edit port1
      set ip 169.254.3.1 255.255.255.0
```

```
      set allowaccess capwap ping
      set auto-auth-extension-device enable
   end
end
```

3. Configure an NTP server on port 1.

```
config system ntp
   set server-mode enable
   set interface port1
end
```

4. Authorize the FortiSwitch unit as a managed switch.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      set fsw-wan1-admin enable
   end
end
NOTE: FortiSwitch will reboot when you issue the above command.
```

5. Configure a DHCP server on port 1.

```
config system dhcp server
   edit 0
      set ntp-service local
      set default-gateway 169.254.3.1
      set netmask 255.255.255.0
      set interface port1
      config ip-range
         edit 0
            set start-ip 169.254.3.2
            set end-ip 169.254.3.254
         end
      set vci-match enable
      set vci-string FortiAP FortiSwitch FortiExtender
   end
end
```

# Configuring FortiLink (LAG)

Starting in FortiSwitchOS 3.3.0, you can configure the FortiLink as a Link Aggregation Group (LAG) to provide increased FortiLink bandwidth between the FortiGate and FortiSwitch.

**NOTE**: LAG is supported on all FortiSwitch models and on FortiGate models FGT-100D and above.

Connect any of the FortiLink-capable ports on the FortiGate to the FortiSwitch. Make sure that you configure auto-discovery on the FortiSwitch ports (unless the port is a default auto-discovery port).

## Configuring the switch

No additional switch configuration is required for the LAG.

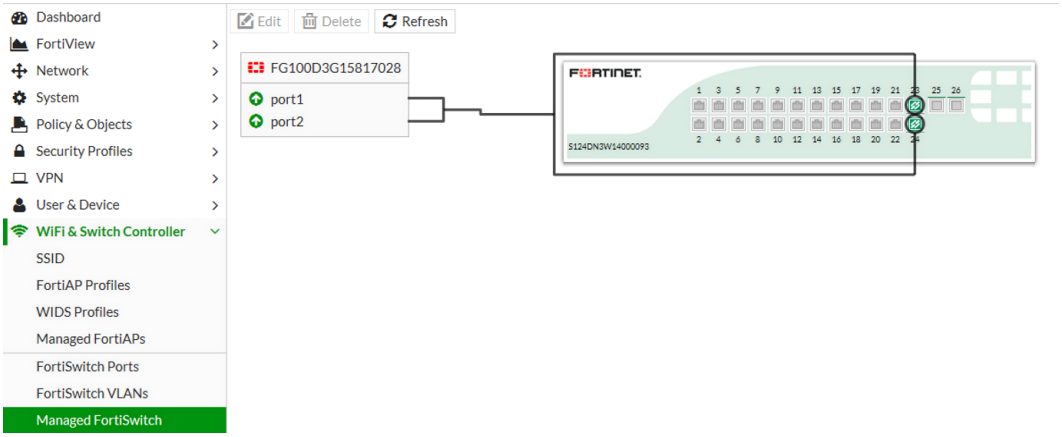
## Configuring the LAG on the FortiGate

1. Go to **Network> Interfaces**
2. (Optional) If the FortiLink physical ports are currently included in the internal interface, edit the internal interface and remove the desired ports from the Physical Interface Members.
3. Click **Create New**
4. Enter the following fields in the **Add Interface** form:
   a. **Interface name**: enter a name for the interface (such as "fortilink")
   b. **Type**: select **FortiLink**
   c. **Physical Interface Members** : select the ports for the LAG
   d. **IP/Network Mask**: system automatically sets the IP address and network mask.
   e. Administrative Access: check the boxes for **ping, capwap, http** and **https**.
5. Go to **WiFi & Switch Controller** > **Managed Devices** > **Managed FortiSwitch**. Click on the switch faceplate and select **Authorize**.
6. From the FortiGate CLI, ensure that NTP is enabled for the FortiLink LAG:

```
config system ntp
   set server-mode enable
   set interface fortilink
end
```

The following image shows the Managed FortiSwitch display. The page displays the FortiGate ports on the left, and the faceplate for each FortiSwitch on the right. The link between the FortiSwitch and FortiGate splits at each end to indicate which ports are members of the LAG.

Before the LAG becomes established, the FortiLink is displayed with dashed lines with a broken-link icon. When the FortiLink LAG is established successfully, the port status for the LAG ports is green (on the FortiGate port list and on the FortiSwitch faceplate), and the link between the ports is a solid line.




### Network Interface Display

In **System** > **Network** > **Interfaces**, the system displays the switch ID next to the interface name, and displays **Dedicated to Extension Device** in the IP/Netmask field .

**Note**: An interface configured for managed FortiAP is also set to **Dedicated to Extension Device**. Make sure that you are viewing the correct FortiLink interface.

## Using the FortiGate CLI

### Configuring the LAG on the FortiGate

To configure the FortiLink as a LAG, create a FortiLink interface on the FortiGate, add the physical ports, and authorize the FortiSwitch as a managed switch. In the following steps, port4 and port5 are configured as the FortiLink LAG.

1. If required, remove the LAG ports from the **lan** interface:

```
config system virtual-switch
   edit lan
      config port
         delete port4 port5
      end
   end
end
```

2. Create a trunk (of type fortilink) with the two ports that you connected to the switch:

```
config system interface
   edit fortilink
      set allowaccess ping capwap https
      set type fortilink
      set member port4 port5
      set lacp-mode static
   next
end
```

3. Configure an NTP server on the LAG interface:

```
config system ntp
   set server-mode enable
   set interface fortilink
end
```

4. Authorize the FortiSwitch unit as a managed switch.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      set fsw-wan1-admin enable
   end
end
NOTE: FortiSwitch will reboot when you issue the above command.
```

5. Configure a DHCP server on port 1.

```
config system dhcp server
   edit 0
      set ntp-service local
      set netmask 255.255.255.252
      set interface fortilink
      config ip-range
         edit 1
            set start-ip 169.254.254.2
            set end-ip 169.254.254.2
         end
      set vci-match enable
      set vci-string FortiSwitch
```

```
    end
  end
```

### Configuring the switch

No switch configuration is required for the LAG.

## Configuring FortiSwitch Management Port

If the FortiSwitch model has a dedicated management port, you can configure remote management to the FortiSwitch. In FortiLink mode, the FortiGate is the default gateway, so you need to configure an explicit route for the FortiSwitch management port.

### Using the FortiSwitch Web-based Manager

1. Go to **Routing**
2. Under **Static Routes**, click **Create New**
3. Enter the following fields in the **New Static Route** form:
   a. Destination: enter a subnetwork and mask
   b. Device: select the management interface
   c. Gateway: enter the gateway IP address

### Using the FortiSwitch CLI

Enter the following commands:

```
config router static
  edit 1
    set device mgmt
    set gateway <router IP address>
    set dst <router subnet> <subnet mask>
  end
end
```

In the following example, the FortiSwitch management port is connected to a router with IP address 192.168.0.10:

```
config router static
  edit 1
    set device mgmt
    set gateway 192.168.0.10
    set dst 192.168.0.0 255.255.0.0
  end
end
```

## Converting to FortiSwitch Standalone Mode

If a FortiSwitch is operating in managed mode, follow these instructions to convert it to standalone mode.

1. From the switch CLI:

```
config system global
   set mgmt-mode local
end
NOTE: FortiSwitch will reboot when you issue the above command.
```

2. From the FortiGate, use the web-based manager or CLI to perform the following commands before the switch reboot has completed:

**Using the Web-based manager**

a. Navigate to **WiFi & Switch Controller** > **Managed FortiSwitch**.

b. Right-click on the switch and select **De-authorize**.

**Using the CLI**

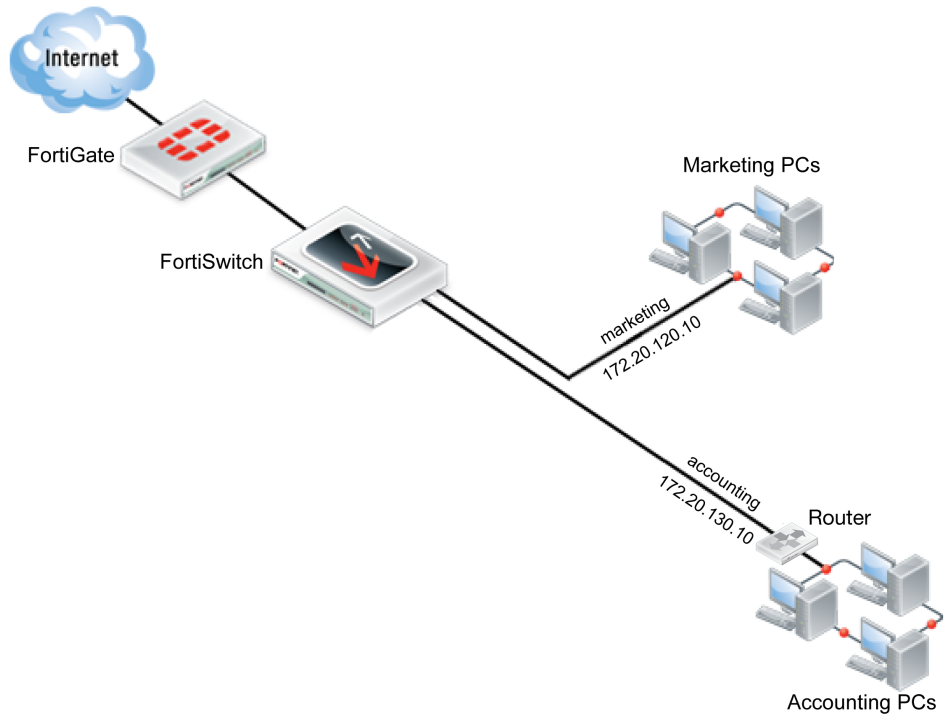
```
config switch-controller managed-switch
   edit <switch-id>
      set fsw-wan1-admin disable
   end
end
```

As an alternative to step 2, you can disconnect the FortiLink cable from the switch and the FortiGate.

# VLAN Configuration

Use Virtual Local Area Networks (VLANs) to logically separate a LAN into smaller broadcast domains. VLANs allow you to define different policies for different types of users and to set finer control on the LAN traffic (traffic is only sent automatically within the VLAN. You must configure routing for traffic between VLANs).

For example, if a company has one LAN which is to be used for both the marketing and the accounting department, this LAN can be segmented into two VLANs. This allows the traffic from each department to be isolated, so information packets sent to the marketing department are only sent on the marketing VLAN. It also allowed different policies to be created, so that security can be increased for the accounting department without also increasing it for the marketing department.



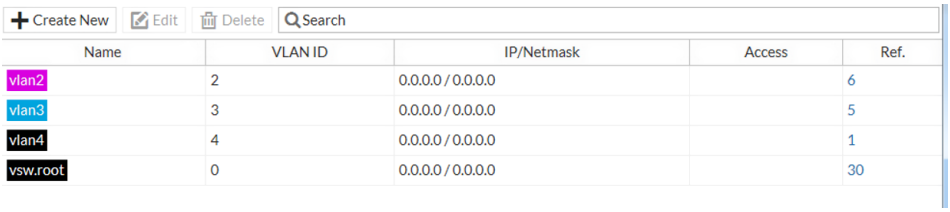

For FortiSwitches managed by the FortiGate unit, you can configure and manage the FortiSwitch VLANs using the FortiGate.

**Note**: in FortiSwitchOS 3.3.0 and later releases, the FortiSwitch supports untagged and tagged frames in Fortilink mode. The switch supports up to 1023 user-defined VLANs. The user can assign a VLAN number (in the range 1-4095) to each of the VLANs.

# FortiSwitch VLANs Display

The **WiFi & Switch Controller** > **FortiSwitch VLANs** page displays VLAN information for the managed switches.

The following figure shows the VLAN page:




Each entry in the VLAN list displays the following information:

- **Name** - name of the VLAN
- **VLAN ID** - the VLAN number.
- **IP/Netmask** - Address and mask of the subnetwork that corresponds to this VLAN
- **Access**
- **Ref** - how many interfaces reference this VLAN.

# Creating VLANs

Setting up a VLAN requires:

- Creating the VLAN.
- Assigning FortiSwitch ports to the VLAN.

The following instructions will create a VLAN to be used by the marketing team for network and Internet access. The marketing team PCs will connect to ports 3-6 on the FortiSwitch.

## Using the web-based manager

### Creating the VLAN

1. Go to **WiFi & Switch Controller** > **FortiSwitch VLANs** and select **Create New**. Change the following settings:

| | |
|---|---|
| **Interface Name** | marketing |
| **VLAN ID** | Enter a number (1-4094) |
| **Color** | Choose a unique color for each VLAN, for ease of visual display. |
| **IP/Network Mask** | 172.20.120.10/255.255.255.0 |

1. Enable **DHCP Server.** Set the IP range to 172.20.120.11-172.20.120.254.
2. Select **OK**.

The entry **marketing** is now shown on the list of **VLANs**. A **marketing** interface has also been added, which can be seen by going to **Network > Interfaces**.

### Assigning FortiSwitch Ports to the VLAN

1. Go to **WiFi & Switch Controller** > **FortiSwitch Ports**
2. Click the rows for ports 3-6 to select them.
3. Right-click and select the VLAN from **Assign VLANS** > **Native VLAN** list.

Ports 3-6 on the FortiSwitch have now been assigned to the marketing VLAN and will appear in red.

## Using the CLI

1. Create the marketing VLAN.

```
config switch-controller vlan
   edit marketing
      set vlanid 4
      set color 32
end
```

2. Set the VLAN's IP address.

```
config system interface
   edit marketing
      set ip 172.20.120.14 255.255.255.0
end
```

3. Enable a DHCP Server.

```
config system dhcp server
   edit 1
      set default-gateway 172.20.120.10
      set dns-service default
      set interface marketing
         config ip-range
            set start-ip 172.20.120.11
            set end-ip 172.20.120.254
         end
      set netmask 255.255.255.0
end
```

4. Assign ports 3-6 to the VLAN.

```
config switch-controller managed-switch
   edit FS224D3W14000370
      config ports
         edit port3
            set vlan marketing
         next
         edit port4
            set vlan marketing
         next
         edit port5
            set vlan marketing
         next
         edit port6
            set vlan marketing
      end
```

```
end
```

# Setting up a security policy for the VLAN

The following instructions configure a basic security policy for the marketing VLAN that will allow all traffic from the marketing VLAN to have access to the Internet.

## Using the web-based manager

1. Go to **Policy & Objects** > **IPv4 Policy** and select **Create New**. Change the following settings:

| | |
|---|---|
| **Incoming Interface** | marketing |
| **Source** | all |
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | ALL |
| **Action** | ACCEPT |
| **Enable NAT** | Enable |
| **Fixed Port** | |
| **IP Pool Configuration** | |
| **Security Profiles** | |
| **Logging Options** | Log all Sessions |

2. Select **OK**.

With this security policy in place, all computers connected to the marketing VLAN can now access the Internet.

## Using the CLI

Create a security policy for the marketing VLAN.

```
config security policy
   edit 2
      set srcintf marketing
      set dstintf wan1
      set srcaddr all
      set dstaddr all
      set action accept
      set schedule always
      set service ALL
```

```
        set logtraffic all
        set nat enable
    end
```

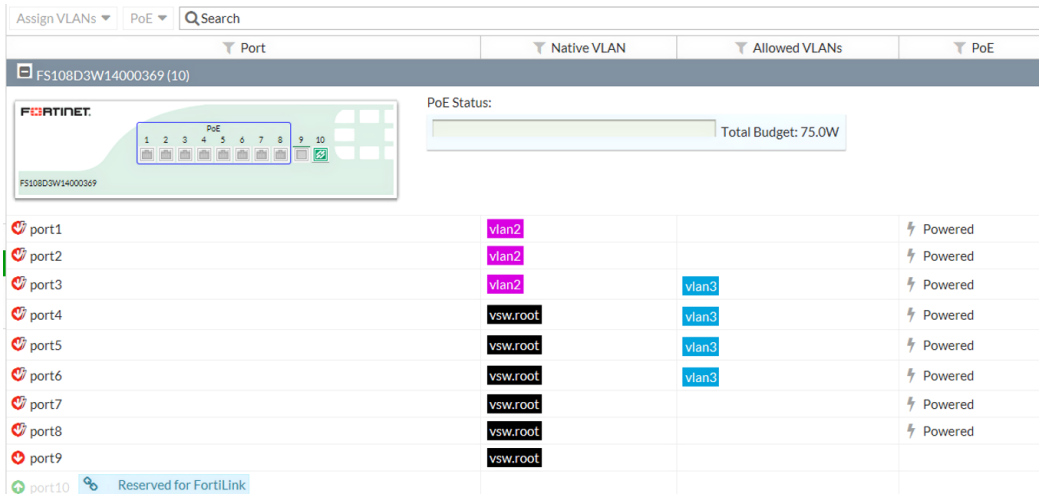
# FortiSwitch Port and POE Configuration

You can configure the FortiSwitch port and POE settings from the FortiGate using the FortiGate web-based manager or CLI commands.

## FortiSwitch Ports Display

The **WiFi & Switch Controller** > **FortiSwitch Ports** page displays port information about each of the managed switches.

The following figure shows the display for a FortiSwitch 108D-POE:

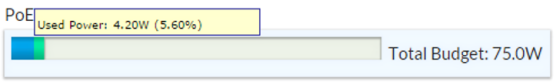


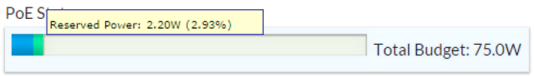

The switch faceplate displays:

- the active ports (green)
- the POE-enabled ports (blue rectangle)
- the FortiLink port (link icon)

The POE Status displays the total power budget, and the actual power currently allocated.

The allocated power displays a blue bar for the used power (currently being consumed) and a green bar for the reserved power (power available for additional devices on the POE ports). See the following figures:



Each entry in the port list displays the following information:

- Port status (red for down, green for up)
- Port name
- Native VLAN
- Allowed VLANs
- POE status

# Configuring Ports Using the Web Manager

You can configure the following for each port:

- Configure Native VLAN on the port
- Configure Allowed VLANs on the port
- Enable or Disable the POE power on a port

## Configure Native VLAN on a port

Follow these instructions to configure VLANs on a port:

1. Navigate to **WiFi & Switch Controller** > **FortiSwitch Ports**
2. Click on a row to select the port.
3. Right-click the row and select **Assign VLANs** > **Native VLAN** and select the desired VLAN.

## Configure Allowed VLANs on a port

Follow these instructions to configure VLANs on a port:

1. Navigate to **WiFi & Switch Controller** > **FortiSwitch Ports**
2. Click on a row to select the port.
3. Right-click the row and select **Assign VLANs** > **Allowed VLANs**
4. In the dialog box, select the desired VLAN. Click the **+** icon to create additional selections.
5. Click **Save Allowed VLANs**.

## Enable or Disable POE on a port

Follow these instructions to configure VLANs on a port:

1. Navigate to **WiFi & Switch Controller** > **FortiSwitch Ports**
2. Click on a row to select the port.
3. Right-click the row, select **POE** and select **Enable POE** or **Disable POE**

**Note**: when you select a row in the port table, you can also use the **Assign VLANs** and **PoE** menus (located just below the page banner), instead of the right-click menu, to configure the values.

# Configuring Ports Using the CLI

The following port CLI commands are available:

- Set port speed.
- Set port admin status
- Configure vlan on the port
- Enable or Disable the POE power on a per-port basis (available starting in FortiSwitchOS 3.3.0)

## Port commands

```
config switch-controller managed-switch
   edit <switch>
      config ports
         edit <port>
            speed <speed>
            status {down | up}
            vlan <vlan_id>
            poe-status {enable | disable}
```

## POE commands

The following POE CLI commands are available starting in FortiSwitchOS 3.3.0:

- Reset any POE port (by toggling the power OFF and then ON)
- Display general POE status

### Reset any POE port (by toggling the power OFF and then ON)

```
execute switch-controller poe-reset <fortiswitch-id> <port>
```

### Display general POE status

```
get switch-controller <fortiswitch-id> <port>
```

The following example displays the POE status for port 6 on the specified switch:

```
# get switch-controller poe FS108D3W14000967 port6
Port(6) Power:3.90W, Power-Status: Delivering Power
Power-Up Mode: Normal Mode
Remote Power Device Type: IEEE802.3AT PD
Power Class: 4
Defined Max Power: 30.0W, Priority:3
Voltage: 54.00V
Current: 78mA
```

# Configuring FortiLink for FortiGate HA

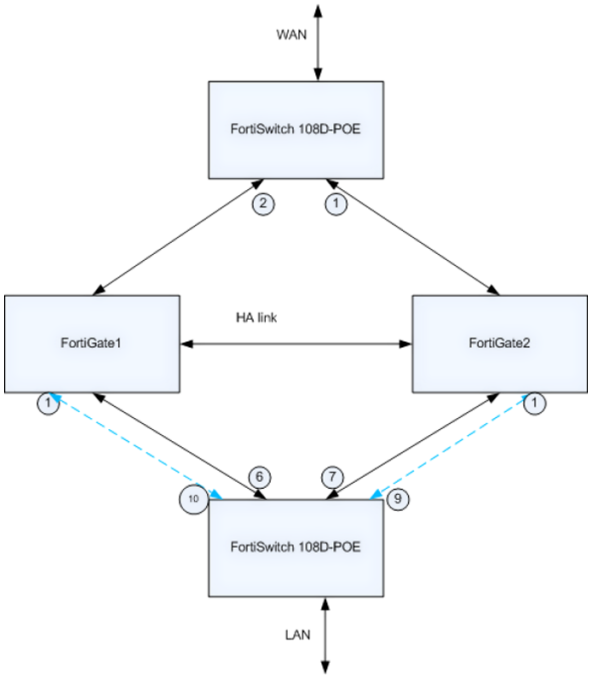
With FortiOS 5.4.0 and later releases, a FortiGate operating in HA mode can use FortiLink (to FortiSwitches running FortiSwitchOS 3.3.0 or later release).

To use FortiLink mode with a pair of FortiGate units in a high-availability cluster, you must connect FortiLink from the switch to both of the FortiGate units.

Highlights of this configuration:

1. No console port or direct management is required on the FortiSwitch.
2. All the actions described here can be performed from FortiCloud if needed
3. All FortiSwitch internal state and counters are visible when in FortiLink managed mode

## Example Topology




The LAN and WAN links connect to FortiSwitch ports. The FortiSwitch connects to the active and standby FortiGate units. If the standby FortiGate (for example, FGT2) becomes active, this is transparent to the LAN and WAN ports. FortiLink is automatically established to FGT2, and the active traffic path becomes LAN <-> FGT2<-> WAN.

Note the following points:

1. FortiSwitch connects with FortiLink to both of the FortiGate units. These connections can be LAGs (in FortiSwitch 3.3.0 and later releases).
2. LAN and WAN links can connect to separate FortiSwitches, as shown in the figure, or they can connect to the same FortiSwitch.

3. Connect the FortiLinks from any two FortiSwitch ports to FGT1 port X and FGT2 port X, where the FortiGate port numbers must match (port1 in the above topology diagram).
4. For FortiLink LAGs, connect Fortilinks from two additional FortiSwitch ports to FGT1 port Y and FGT2 port Y, where the FortiGate port numbers must match.

## Adding a Second FortiGate to Existing Single FortiGate

Connect an additional FortiLink from the FortiSwitch to the new FortiGate, and configure HA on both of the FortiGate units.

### Configuration Steps

Configuration consists of the following major steps:

1. Configure “auto-discovery-fortilink enable” on the FortiSwitch ports that you will connect to FGT2. This step is not required if the port is auto-fortilink by default.
2. Add cable connections from FGT2 to all FortiSwitches (exact duplicate of FGT1 to the FortiSwitches)
3. Connect HA cables between FGT1 and FGT2
4. At FGT1: configure FortiGate High Availability using the GUI. For additional information, refer to the High Availability chapter in the FortiOS Handbook.
5. At FGT2: Configure FortiGate High Availability using the CLI from the console port. The following parameters must be identical to FGT1:
   - HA-mode
   - Priority
   - Group Name and Password
6. At this point, the FGT1 synchronizes with FGT2. This takes several minutes.
7. Verify the configuration at FGT2 using the following commands:

```
get ha status
get system ha status
```

## Adding a Switch to Existing HA FortiGates (single FortiLinks)

Connect one FortiSwitch port to each of the FortiGate units. On FGT1, follow the same FortiLink configuration steps as for the non-HA configuration. FGT1 synchronizes the configuration with FGT2.

### Configuration Steps

1. Configure two FortiSwitch ports as “auto-discovery-fortilink enable”. This step is not required for any port is auto-fortilink by default.
2. Connect one port to FGT1 and the other port to FGT2.
   - The FGT1 and FGT2 port numbers must be identical For example:
   - FortiSwitch port21 and port22 connect to FGT1 port4 and FGT2 port4
3. At FGT1, perform the steps to configure FortiLink (as described in Initial Set-up):
   a. Change an internal port to be the FortiLink port
   b. Authorize the FortiSwitch

4. At FGT2, run the command "get switch-controller managed-switch" to verify that the FGT1 configuration was synchronized successfully

## Adding a Switch to Existing FGT HA setup (Fortilink LAGs)

In this configuration, connect two FortiSwitch ports to each FortiGate unit. Enter the configuration commands on FGT1 (same commands as for the non-HA configuration). The HA feature synchronizes the configuration to FGT2.

### Configuration Steps

1. Configure four FortiSwitch ports as “auto-discovery-fortilink enable”. This step is not required for any port is auto-fortilink by default.
2. Connect two ports to FGT1 and the other ports to FGT2
   - the FGT1 and FGT2 port numbers must be the same. For example:
   - FortiSwitch port21 and port22 connect to FGT1 port4 and port5 and FortiSwitch port23 and port24 connect to FGT2 port4 and port5
3. At FGT1, configure the Fortilink LAG (as described in Initial Set-up):
   a. Create the FortiLink LAG interface and add the physical ports as members
   b. Authorize the FortiSwitch
4. At FGT2, run command "get switch-controller managed-switch" to verify that the FGT1 configuration was synchronized successfully

## Create VLANs for LAN and WAN ports

To connect the LAN and WAN ports to the same FortiSwitch, assign different VLANs to the LAN and WAN ports to separate the traffic.

See FortiSwitch Port and POE Configuration for information about configuring VLANs on FortiSwitch ports.

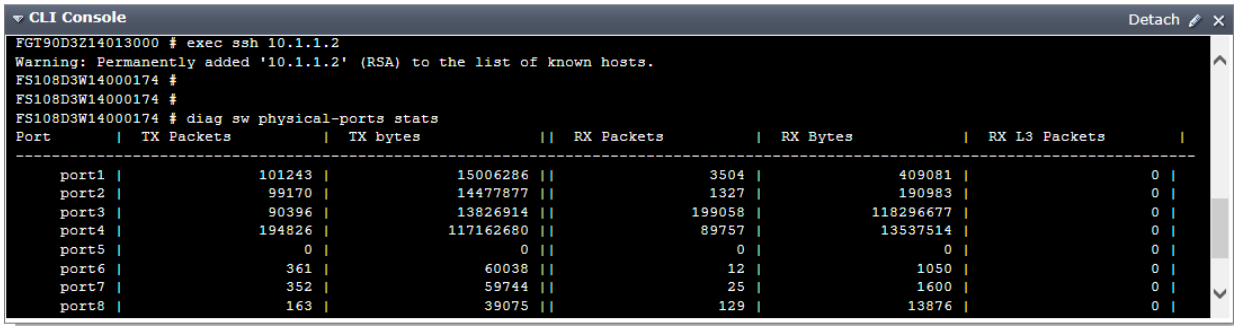
## Test the HA Capability

1. Disconnect power from FGT1 to simulate failure
2. From the FGT2 UI:
   Check **Wifi and Switch Controller** > **Managed FortiSwitch**
3. FortiSwitch is now visible from the management interface on FGT2

## Display FortiSwitch Port Statistics

To display port statistics on the FortiSwitch, execute the following commands from the FortiGate CLI:

```
exec ssh 10.1.1.2
diag sw physical-ports stats
```


CLI Console
Detach
FGT90D3Z14013000 # exec ssh 10.1.1.2
Warning: Permanently added '10.1.1.2' (RSA) to the list of known hosts.
FS108D3W14000174 #
FS108D3W14000174 #
FS108D3W14000174 # diag sw physical-ports stats
Port | TX Packets | TX bytes || RX Packets | RX Bytes | RX L3 Packets |
port1 | 101243 | 15006286 || 3504 | 409081 | 0 |
port2 | 99170 | 14477877 || 1327 | 190983 | 0 |
port3 | 90396 | 13826914 || 199058 | 118296677 | 0 |
port4 | 194826 | 117162680 || 89757 | 13537514 | 0 |
port5 | 0 | 0 || 0 | 0 | 0 |
port6 | 361 | 60038 || 12 | 1050 | 0 |
port7 | 352 | 59744 || 25 | 1600 | 0 |
port8 | 163 | 39075 || 129 | 13876 | 0 |

# Troubleshooting

If the FortiGate does not establish the Fortilink connection with the switch, perform the following troubleshooting checks.

## Troubleshooting FortiLink Issues

### Check the FortiGate configuration

Using the FortiGate GUI, check the FortiLink interface configuration:

1. In **Network** > **Interfaces**, double-click the interface used for FortiLink.
2. Ensure that **Dedicated to Extension Device** is set for this interface.

Using the FortiGate CLI, Verify that you have configured the DHCP and NTP settings correctly. Enter the following commands:

1. Verify that the NTP server is enabled, and the Fortilink interface has been added to the list:

```
show system ntp
```

2. Ensure that the DHCP server on the Fortilink interface is configured correctly:

```
show system dhcp
```

### Check the FortiSwitch configuration

Use the following FortiSwitch CLI commands to check the FortiSwitch configuration:

1. Verify that the switch system time matches the time on the FortiGate:

```
get system status
```

2. Verify that FortiGate has sent an IP address to the FortiSwitch.
Typically, the IP address will be in the range of 169.254.x.x:

```
get system interfaces
```

3. Verify that you can ping the FortiGate IP address:

```
exec ping x.x.x.x
```

# Scenarios

This chapter contains practical examples of how to use the FortiSwitch unit to manage a network. The scenarios assume that you have completed the configurations described in the VLAN Configuration chapter.

The scenarios are as follows:

- Scenario 1: Allowing access to specific users on the marketing VLAN
- Scenario 2: Adding a specific device to the marketing VLAN

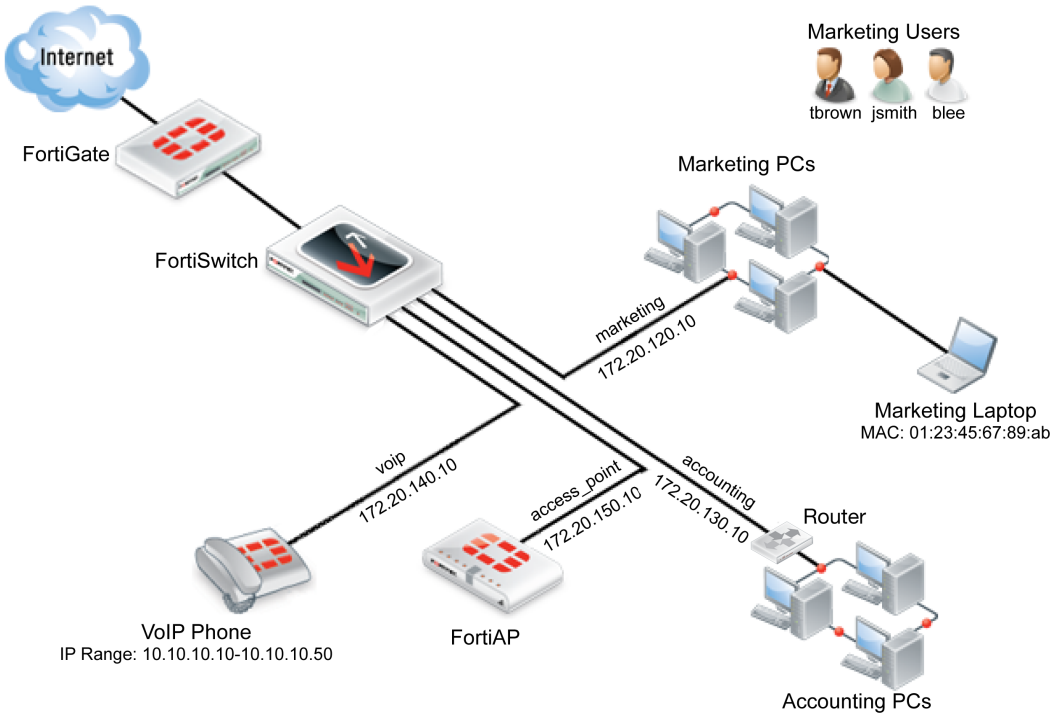
## The Example Network

All the scenarios are interrelated and are used to manage an example network with the following attributes:

- The FortiSwitch unit used is a FortiSwitch-224D-POE, serial number FS224D3W14000370.
- The FortiSwitch unit's port 24 connects to port1 on the FortiGate unit.
- The LAN is divided into four distinct VLANs, configured as follows:

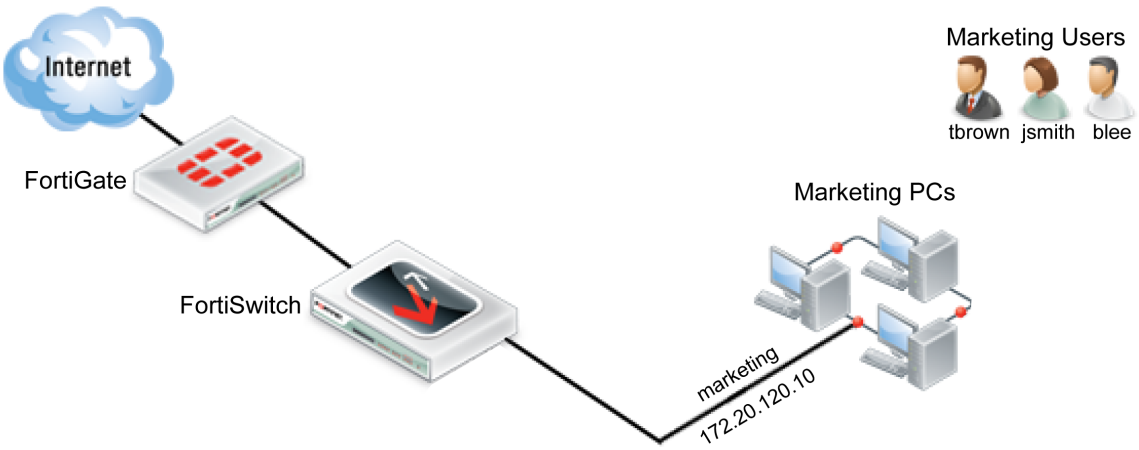
| VLAN | IP | Device(s) | Port(s) | Policy ID(s) | GUI Color |
|---|---|---|---|---|---|
| marketing | 172.20.120.10/255.255.255.0 | marketing PCs, marketing laptop | 3-6 | 2, 3 | |
| accounting | 172.20.130.10/255.255.255.0 | accounting PCs | 21 | 4 | |
| voip | 172.20.140.10/255.255.255.0 | VoIP phone | 10 | 5 | |
| access_ point | 172.20.150.10/255.255.255.0 | FortiAP | 1 | 6 | |

- There are six devices that connect directly to the FortiSwitch unit's ports using Ethernet cables: the 3 marketing PCs, the marketing laptop, the VoIP phone, and the FortiAP unit.
- The accounting VLAN connects to the FortiSwitch using an SFP port.
- There are three marketing employees (Jane Smith, Tom Brown, Bob Lee) who will use the marketing VLAN using the marketing PCs.
- The MAC address of the marketing laptop is 01:23:45:67:89:ab.
- The IP range for the VoIP phone is 10.10.10.10-10.10.10.50.
- The FortiAP unit is a FortiAP-11C, serial number FAP11C3X12000412.




## Scenario 1: Allowing access to specific users on the marketing VLAN

In Scenario 1, the policy for the marketing VLAN will be altered so that different users have different access. The firewall policy will be created so that all three marketing employees (Jane Smith, Tom Brown, Bob Lee) have user accounts. These accounts will be put into one of two groups: full-time and part-time. Full-time employees will always have network access, while part-time employees will only have access on Mondays, Wednesdays and Fridays. This policy will apply to each user when they use any of the PCs that connect to the marketing VLAN through ports 3, 4, 5 or 6 on the FortiSwitch.



Creating a policy to match scenario 1 requires:

- Creating users.
- Creating groups.
- Creating a schedule.
- Configuring the firewall policies.

## Using the web-based manager

### Creating a User Group

1. Go to **User & Device** > **User Groups** and select **Create New**.
2. Name the user group **part-time**.
3. Set **Type** as **Firewall**.
4. Select **OK**.

The entry **part-time** will now appear on the user group list. Repeat these steps to create another user group, named **full-time**.

### Creating a User

1. Go to **User & Device** > **User Definition**. Select **Create New**.
2. Use the **User Creation Wizard** to create a user. In part 1, select **Local User**.
3. In part 2, change the following settings:

| | |
|---|---|
| **User Name** | blee |
| **Password** | password |

4. In part 3, enter the email address blee@example.com
5. In part 4, select **Enable** and **User Group**. Set **part-time** as the group.
6. Select **Done**.

The entry **blee** will now appear in the user list. Repeat these steps to create user accounts **tbrown** and **jsmith** and add both of these accounts to the **full-time group.**

### Creating a Schedule

1. Go to **Policy & Objects** > **Schedules**. Select **Create New** and then select **Recurring**.
2. Change the following settings:

| | |
|---|---|
| **Name** | part-time_schedule |
| **Day of the Week** | Monday, Wednesday, Friday |

3. Select **OK**.

The entry **part-time schedule** will now appear on the schedules list.

### Configuring the Firewall Policy

1. Go to **Policy & Objects** > **IPv4 Policy** and select the policy for the marketing VLAN. Select **Edit**.
2. Set the policy to use the following the following settings, allowing access for part-time employees:

| | |
|---|---|
| **Incoming Interface** | marketing |
| **Source Address** | all |
| **Source User(s)** | part-time |
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | part-time_schedule |
| **Service** | ALL |
| **Action** | ACCEPT |
| **Enable NAT** | Enable |
| **Logging Options** | Log all Sessions |

3. Select **OK**.
4. Go to **Policy & Objects** > **IPv4 Policy** and create a new policy.
5. Change the following settings to set access for full-time employees:

| | |
|---|---|
| **Incoming Interface** | marketing |
| **Source Address** | all |
| **Source User(s)** | full-time |
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | ALL |
| **Action** | ACCEPT |
| **Enable NAT** | Enable |
| **Logging Options** | Log all Sessions |

6. Select **OK**.

You have now finished creating the policies that matches scenario 1. These policies will apply to all three users when they use any of the PCs that connect to the marketing VLAN.

## Using the CLI

1. Create the 3 users.

```
config user local
   edit blee
      set type password
      set passwd password
   next
   edit tbrown
      set type password
      set passwd password
   next
   edit jsmith
      set type password
      set passwd password
end
```

2. Create the 2 user groups and add the users to them.

```
config user group
   edit part-time
      set group-type firewall
      set member blee
next
   edit full-time
      set group-type firewall
      set member tbrown jsmith
end
```

3. Create the schedule for part-time employees.

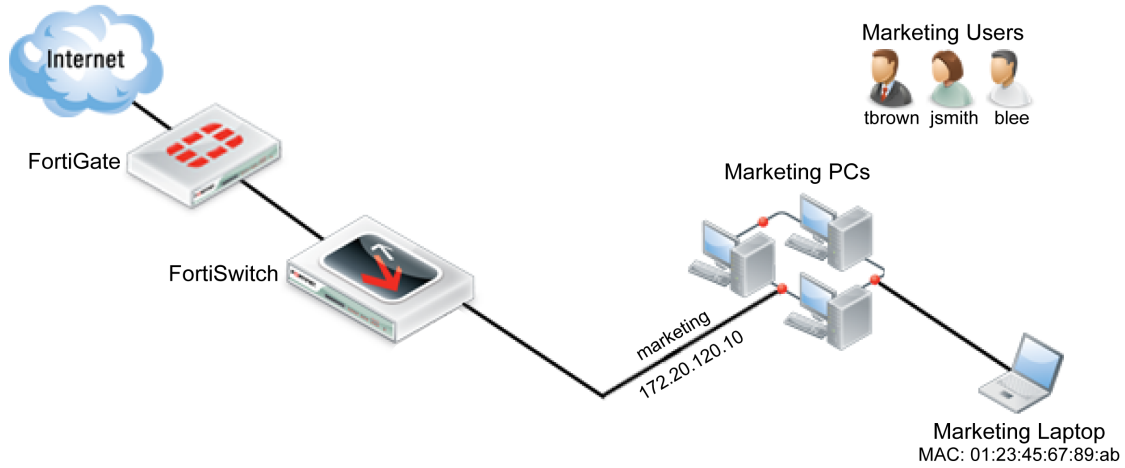
```
config firewall schedule recurring
   edit part-time_schedule
      set day monday wednesday friday
end
```

4. Add user authentication to the firewall policy for the marketing VLAN.

```
config firewall policy
   edit 2
      set identity-based enable
         config identity-based-policy
            edit 1
               set schedule part-time_schedule
               set logtraffic all
               set groups part-time
               set dstaddr all
               set service ALL
            next
            edit 2
               set schedule always
               set logtraffic all
               set groups full-time
               set dstaddr all
               set service ALL
         end
end
```

# Scenario 2: Adding a specific device to the marketing VLAN

In Scenario 2, a new policy will be created for the marketing VLAN that will be used by the marketing laptop. This policy will affect the marketing laptop that is used periodically for tasks such as boardroom presentations or for guests, tasks for which the laptop requires Internet access. The laptop will access the Internet by connecting to the marketing VLAN through ports 3, 4, 5 or 6 on the FortiSwitch. Adding a new policy for the laptop will allow it to connect without requiring user authentication and will also limit the scope of the device's access.




Creating a policy to match scenario 2 requires:

- Assigning a reserve IP to the laptop.
- Creating a firewall address for the reserve IP.
- Creating a firewall policy that uses the reserve IP.

## Using the web-based manager

### Assigning a Reserve IP to the Laptop

1. Go to **Network > Interfaces** and select **marketing**.
2. Under **DHCP Server**, expand the **Advanced** options.
3. In the **MAC Address Access Control List** and select **Create New**.
4. Change the following settings:

| | |
|---|---|
| **MAC** | 01:23:45:67:89:ab |
| **IP** | 172.20.120.254 |
| **Action** | Reserve IP |

### Creating a Firewall Address for the Reserve IP

1. Go to **Policy & Objects > Addresses** and select **Create New**.
2. Change the following settings:

| | |
|---|---|
| **Category** | Address |
| **Name** | marketing_laptop |
| **Type** | IP/Netmask |
| **Subnet/IP Range** | 172.20.120.254 |
| **Interface** | marketing |

### Configuring a Firewall Policy

1. Go to **Policy & Objects > IPv4 Policy** and select **Create New**.
2. Change the following settings:

| | |
|---|---|
| **Incoming Interface** | marketing |
| **Source Address** | marketing_laptop |
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | HTTP HTTPS DNS |
| **Action** | ACCEPT |
| **Enable NAT** | Enabled |
| **Logging Options** | Log all Sessions |

3. Select **OK.**
4. In the policy list, select the column on the far left for the new policy (usually **Seq #)** and drag the policy above the previous policy for the marketing VLAN. This will ensure that the laptop will be identified through this policy.

You have now finished creating a policy that matches scenario 2. This policy will apply to anyone who uses the laptop to connect to the **marketing** VLAN using an Ethernet cable.

## Using the CLI

1. Assign a reserve IP to the laptop.

```
config system dhcp server
   edit 2
      config reserved-address
         edit 1
            set action reserved
            set ip 172.20.120.254
            set mac 01:23:45:67:89:ab
      end
end
```

2. Create a firewall address for the reserve IP.

```
config firewall address
   edit marketing_laptop
      set subnet 172.20.120.254
end
```

3. Create a firewall policy for the marketing VLAN that uses the reserve IP.

```
config firewall policy
   edit 3
      set srcintf marketing
      set dstintf wan1
      set srcaddr marketing_laptop
      set dstaddr all
      set action accept
      set schedule always
      set service HTTP HTTPS DNS
      set logtraffic all
      set nat enable
end
```

4. Place the new firewall policy at the top of the policy list.

```
config firewall policy
   move 2 after 3
end
```

| | |
|---|---|
| **Address Name** | marketing VLAN |
| **Type** | Subnet |
| **Subnet/IP Range** | 172.20.120.14/255.255.255.0 |
| **Interface** | marketing |

| | |
|---|---|
| **Name** | marketing-remote |
| **Enable Tunnel Mode** | Enable |
| **Enable Split Tunneling** | Disable |
| **IP Pools** | SSLVPN_TUNNEL_ADDR1 |
| **Enable Web Mode** | Enable |

| | |
|---|---|
| **Incoming Interface** | ssl.root (sslvpn tunnel interface) |
| **Source Address** | marketing_laptop |
| **Outgoing Interface** | marketing |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | ALL |

| | |
|---|---|
| **Action** | ACCEPT |
| **Enable NAT** | Enabled |
| **Logging Options** | Log all Sessions |

| | |
|---|---|
| **Incoming Interface** | ssl.root (sslvpn tunnel interface) |
| **Source Address** | marketing_laptop |
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | HTTP HTTPS DNS |
| **Action** | ACCEPT |
| **Enable NAT** | Enabled |
| **Logging Options** | Log all Sessions |

The FortiClient SSL VPN tunnel client will also need to be configured, in order for the Tom Brown to connect to the SSL VPN tunnel.

The SFP ports should only be used to connect UL-listed optical transceiver products, rated Laser Class 1.33V DC.

SFP ports are only available on certain FortiSwitch models. SFP ports are also shared with Ethernet ports and so when an SFP port is used, the Ethernet port with the same number cannot be.

| | |
|---|---|
| **Name** | accounting |
| **Color** | |
| **IP/Network Mask** | 172.20.130.15/255.255.255.0 |

| | |
|---|---|
| **Incoming Interface** | accounting |
| **Source Address** | all |

| | |
|---|---|
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | ALL |
| **Action** | ACCEPT |
| **Enable NAT** | Enabled |
| **Logging Options** | Log all Sessions |

| | |
|---|---|
| **Name** | voip |
| **Color** | |
| **IP/Network Mask** | 172.20.140.16/255.255.255.0 |

| | |
|---|---|
| **Category** | Address |
| **Name** | voip |
| **Color** | |
| **Type** | IP Range |
| **Subnet/IP Range** | 10.10.10.10-10.10.10.50 |
| **Interface** | voip |

| | |
|---|---|
| **Incoming Interface** | voip |
| **Source Address** | voip_phone |
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | SIP |
| **Action** | ACCEPT |
| **Enable NAT** | Enabled |
| **Logging Options** | Log all Sessions |

| | |
|---|---|
| **Name** | access_point |

| | |
|---|---|
| **Color** |  |
| **IP/Network Mask** | 172.20.150.17/255.255.255.0 |
| **DHCP Server** | Enable |

| | |
|---|---|
| **Name** | WLAN |
| **Type** | WiFi SSID |
| **Traffic Mode** | Tunnel to Wireless Controller |
| **IP/Network Mask** | 172.20.150.17/255.255.255.0 |
| **DHCP Server** | Enabled |
| **SSID** | wireless |
| **Pre-shared Key** | password |

| | |
|---|---|
| **Incoming Interface** | access_point |
| **Outgoing Interface** | wan1 |
| **Destination Address** | all |
| **Schedule** | always |
| **Service** | HTTP HTTPS DNS |
| **Action** | ACCEPT |
| **Enable NAT** | Enabled |
| **Logging Options** | Log all Sessions |




Copyright© 2016 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations,and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.